

Overview and Potential Benefits:

Active Directory Federation Services (ADFS) provides a way to use existing Active Directory (AD) user names and passwords to access “claims-aware” applications that reside in other AD forests or in the cloud. “Claims-aware” applications have been written to recognize and accept access claims passed via ADFS from an external source.

CTS has fielded inquiries about utilizing ADFS in the Enterprise Active Directory (EAD) forest, but business and technical requirements have not been fully defined. Some possible uses suggested include using ADFS to provide use of AD credentials for:

- ArcGIS in the cloud via the GIS Portal
- Microsoft’s Office 365 cloud service
- Department of Fish and Wildlife’s Telecom application by those outside EAD.

Features of ADFS include:

- Allows use of AD identity to access claims-aware applications located in the cloud.
- Allows users in ADFS-enabled forests outside of EAD to access ‘claims aware’ applications deployed inside EAD.
- Provides access to claims-aware applications (such as SharePoint) for EAD users from a home computer using a web interface similar to Outlook Web Application.
- Can provide access control to claims-aware applications by individual AD identity, or by AD-defined security groups. If the claims-aware application accepts AD security group information, then AD administrators will have some ability to control application access rights by choosing which AD security group to associate the user with.

A claims-aware application typically is written to provide ‘same sign-on’ (a separate sign on, but using the user’s existing AD user account and password). Some are written to provide ‘single sign-on’ (no additional sign-on, the user’s credentials are passed directly).

CTS Effort to Deploy and Support:

CTS’ tasks associated with managing and maintaining an ADFS installation would include:

- Installing and managing the ADFS Servers and associated technologies such as the ADFS proxy, firewalls and load-balancers. Based on experience gained during ADFS installation in pre-production EAD, it is estimated that it will take ~~4~~6~~four~~ months to bring up an ADFS infrastructure in the Production EAD Forest.
- Maintaining ADFS in both EAD Production and Pre-production. This would include patching, monitoring, reviewing logs, making sure that the federation trusts are working properly and other administrative tasks to ensure the health of the ADFS infrastructure.
- Working with agencies and vendors to establish federations with claims-aware applications in other forests, or in the cloud.

Agency Support Responsibilities:

- Gather all required information and work with the CTS Administrator to test and implement every new Federation Trust to an external entity. To this end, agencies must maintain an environment in the EAD pre-production forest.
- Agency EAD administrators will manage user access to the application via security groups (if supported by the claims-aware application).
- Development of claims aware applications and federation requirements for any access to be granted to external ADFS-enabled forests.
- Agencies that have not joined the EAD (such as DOT, WSP, LCB, etc.) will need to implement ADFS in their forests. ADFS cannot control multiple forests.
- Schedule Security Design Reviews with CTS Enterprise Security Services (ESS) to ensure that any new federation trusts meet Washington State security policies.

Estimated Costs:

System Cost: A basic ADFS Service would include three ADFS Windows 2008 R2 Servers (2 hardware and 1 Virtual located in a remote site) installed in a “farm”. The native Microsoft Windows Internal Database (WID) would be used. The infrastructure would be built in the EAD Root Domain (wa.lcl) and located in the same network infrastructure as the Exchange 2010 Email Service, using the agency domain controllers and firewalls already deployed for Exchange.

In addition, an environment would be deployed and maintained in the Pre-Production Forest on virtual servers for pilot deployments and QA testing before federation claims are deployed in the Production Forest. It is assumed that access from the internet can be accomplished using the Threat Management Gateway deployed for Exchange 2010.

The estimated cost of the ADFS Service for production (Olympia and Spokane) and pre-production environment is approximately \$2,500 per month.

Support Costs: FTE support costs for ADFS software and the underlying infrastructure are estimated at 48 minutes a day and total approximately \$1,665.00 per month. This does not account for the effort required to establish new Federation Trusts. The support costs may be higher if these prove to be numerous.

Total Costs approximately: \$4,165 per month